



ISO 27001

INFORMATION SECURITY MANAGEMENT

CERTIFIED BY



ISO/IEC 27001 – Information Security Management System

The international standard ISO 27001 describes the requirements for an information security management system (ISMS).

Information security means the protection of information and information systems against unauthorised access, use, disclosure, disruption, modification or destruction. For over twenty years, the most important principles of information security have been (confidentiality, integrity and availability – also known as the ‘CIA triad’). Information Security Management System (ISMS) is part of a general management system in companies and promotes the security of information related to risk management.

An Information Security Management System (ISMS) protects your sensitive data. Aligned with ISO 27001, it provides a structured framework to protect people, processes and IT systems. By implementing an ISMS, you minimise the risks of data breaches, protect your company's reputation and comply with regulations, ultimately protecting your business and image.

Your tailor-made solution

Whether you are a small startup or a large enterprise, information security is of paramount importance.

The principal concept behind an ISMS for an organisation is the design, implementation and maintenance of a coherent totality of processes and systems for the effective management of information accessibility. Just as in the case of all management processes, an ISMS must remain effective and efficient in the long term, and has to be modified in accordance with changes in the internal organisation and the external environment.

ISO 27001 provides a structured approach to managing your organisation's information security risks. By implementing an ISMS, you gain a competitive advantage, improve your brand reputation and build customer trust. This internationally recognised standard promotes a culture of continuous improvement and can be easily integrated with other management systems.

By working with Vincotte, a Kiwa Company, you can effectively manage your security risks, build trust with customers, employees and partners and gain a competitive advantage. Vincotte's expertise extends across the entire ISO 27000 family, including cloud security (ISO 27017), so you can be assured of the support you need to navigate the changing information security landscape.

Your result

The benefits of ISO 27001 certification

- **Protect your information** - by helping you manage risk and improve processes, ISO 27001 allows you to protect your information and that of your customers.
- **Enhance your reputation** - an ISO 27001 certification shows that you have taken steps to protect data, enhancing your reputation.
- **Avoid financial fines** - by managing risk with ISO 27001, you can reduce the likelihood of a data breach and avoid fines.
- **Exchange information securely** - with ISO 27001, you can ensure that your processes are secure enough to exchange sensitive information with customers and partners.
- **Comply with regulations** - ISO 27001 helps ensure you comply with regulations, such as the European Union's General Data Protection Regulation (EU GDPR).
- **Improve competitiveness** - with ISO 27001 certification, you can differentiate yourself from competitors by demonstrating your commitment to security standards.

- **Strengthen your relationships** - with ISO 27001, you can demonstrate that you take customers' and partners' data and information assets seriously.

Please note

Legislations

- Intellectual property rights
- Protection of information about the organisation
- Protection of information and privacy of personal information
- Prevention of misuse of information processing facilities
- Regulation of cryptographic controls

Norms and Standards

ISO/IEC 27001: 2013 Information technology- Security techniques – Information Security Management Systems – Requirements.

In which situation?

Regardless of your industry or size, ISO 27001 provides a robust framework for managing the security of your organisation's critical information.

Whether it is financial data, intellectual property or personnel records - and whether you manage your own or third-party information - ISO 27001 provides a structured approach to identifying, assessing and mitigating information security risks.

Basis for the 27k family:

- ISO/IEC 27002 Information technology – Security techniques – Code for information security
- ISO/IEC 27003 Guide for implementation
- ISO/IEC 27004 ISMS measurements
- ISO/IEC 27005 Risk Management approach
- ISO/IEC 27006 Certification Process
- ISO/IEC 27007 Auditing system
- ISO/IEC 27008 Auditing controls
- ISO/IEC 27011 Guidelines for the telecommunication industry
- ISO/IEC 27013 Integration with ITSMS (Information Technology Service Management Systems)
- ISO/IEC 27014 Governance
- ISO/IEC 27015 Financial and insurance sector
- ISO/IEC 27031 Business continuity
- ISO/IEC 27032 Cyber security
- ISO/IEC 27033 IT network security
- ISO/IEC 27034 Application security